UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/538,556	06/13/2005	Bonnie C. Sexton	US02 0576 Us	5050

65913 7590 07/15/2008

NXP, B.V.
NXP INTELLECTUAL PROPERTY DEPARTMENT
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

NOTIFICATION DATE	DELIVERY MODE
07/15/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	**Application No.** 10/538,556	**Applicant(s)** SEXTON, BONNIE C.
	Examiner MICHAEL PYZOCHA	**Art Unit** 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☒ Claim(s) *4* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 June 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *6/13/05*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-18 are pending.

2. Preliminary amendment filed 06/13/2005 has been received and considered.

Priority

3. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. 119(e) as follows:

The later-filed application must be an application for a patent for an invention which is also disclosed in the prior application (the parent or original nonprovisional application or provisional application). The disclosure of the invention in the parent application and in the later-filed application must be sufficient to comply with the requirements of the first paragraph of 35 U.S.C. 112. See *Transco Products, Inc. v. Performance Contracting, Inc.*, 38 F.3d 551, 32 USPQ2d 1077 (Fed. Cir. 1994).

The disclosure of the prior-filed application, Application No. 60433365, fails to provide adequate support or enablement in the manner provided by the first paragraph of 35 U.S.C. 112 for one or more claims of this application. The provisional application fails to provide an enabling disclosure for claims 1-18 of the present invention as it merely contains ideas the applicant's intend to perform without any explanation how the ideas will be fulfilled. Specifically, each independent claim contains affine and inverse affine transformations which are not even mentioned in Application No. 60433365 and each dependent claim that further limits the invention are additionally not described in 60433365. Therefore, claims 1-18 are not given the priority claimed in Application No. 60433365 to December 13, 2002.

The priority claims to Application No. 60473527 to May 27, 2003 is proper and the claims have been examined with respect to this date.

Information Disclosure Statement

4. The information disclosure statement (IDS) submitted on 06/13/2005 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Objections

5. Claim 4 is objected to because of the following informalities: Claim 4 contains the phrase “either an affine and an inverse affine transformation” to be grammatically correct it should read “either an affine or an inverse affine transformation”. Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claim 3 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

8. Claim 3, contains the terms "b'_n", "b_n" (where n takes the values 0…7) and "$\oplus$" none of these are defined in claim 3 or its intervening claims and therefore each lacks antecedent basis.

Claim Rejections - 35 USC § 101

9. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

10. Claims 1-3 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 1 relates to an apparatus comprising an S-Box constructed by composing a first and second transformation wherein the first transformation is a look-up table and the second transformation is an affine-all transformation. A look-up table is merely data and therefore non-functional descriptive material. While the affine-all transformation is a mathematical algorithm (see specification page 6) thereby making it functional descriptive material. However, the claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the mean of 35 USC §101. Furthermore, even if hardware was added a question of practical application would arise because an S-Box alone does not constitute performing the SubByte function of the Rijndael Block Cipher; the S-Box is in a non-linear transformation. As per claims 2 and 3, each claim recites a portion of

hardware (i.e. combinational logic circuit and ROM) but it is not clear that this hardware is included in the claim or is merely the data created using the hardware.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

12. Claims 1, 4, 5, 9, 10, and 12-15 are rejected under 35 U.S.C. 102(b) as being anticipated by Satoh et al. (“A Compact Rijndael Hardware Architecture with S-Box Optimization” (c) 2001).

As per claims 1, 4, 5, 12 and 14, Satoh et al. discloses an apparatus for encryption and decryption by performing a SubByte function of the Rijndael Block Cipher, comprising: an S-box constructed by composing a first and second transformation, wherein the first transformation is a look-up table for the multiplicative inverse in the finite field GF(2^8), and performing a non-linear byte substitution using the composed S-Box (see page 240 section 2 paragraphs 1 and 2) and the second transformation is, an affine-all transformation that performs both an affine and inverse affine transformation (see page 241-242 section 3.1 where "Enc/Dec block" performs both encryption and decryption by using either the affine transformation or the inverse affine transformation as specifically shown on page 242).

As per claim 9, Satoh et al. discloses the apparatus is arranged to perform encryption or decryption in accordance with the Rijndael Block Cipher, and wherein the data processing module is arranged to implement a Rijndael round (see page 240 section 2 paragraph 1 where this implementation performs 10 rounds).

As per claim 10, Satoh et al. discloses the data processing module is arranged to implement the SubByte transformation of the Rijndael round using the look\- up table composed with the affine transformation for encryption and the inverse affine transformation for decryption (see top of page 242).

As per claims 13 and 15, Satoh et al. discloses means for obtaining the multiplicative inverse is a look-up table and said means for performing the affine-all transformation is a combinational logic circuit (see page 241 section 3.1 where the circuit executes both encryption and decryption and therefore must obtain the look-up table and perform an “affine-all” transformation as further shown on page 242).

Claim Rejections - 35 USC § 103

13. Claims 2, 3, 6, 7, 11, and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Satoh et al. as applied to claims 1, 4, 5, 10 and 14 above, in view of Applicant’s Admitted Prior Art (hereinafter AAPA).

As per claims 2 and 18, Satoh et al. discloses the look-up table is the multiplicative inverse in the finite field GF(2^8) (see page 240 section 2 paragraphs 1 and 2), and the affine-all transformation is implemented using a combinational logic circuit (see page 241 section 3.1 where the circuit executes both encryption and decryption and therefore must obtain the look-up table and perform an "affine-all" transformation as further shown on page 242), but fails to explicitly disclose that in the look-up table has {00} mapped to itself.

However, AAPA teaches mapping {00} to itself (see page 3 lines 17-18).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to map {00} to itself in the Satoh et al. system.

Motivation to do so would have been to conform to the FIPS standard (see AAPA page 3).

As per claims 3, 6, 7, 11, 16 and 17, Satoh et al. fails to explicitly disclose the look-up table is implemented in ROM and the combinational logic circuit implements the equations

$$
\begin{aligned}
b'_0&=[(b_0\cdot p_0)\oplus(b_1\cdot p_1)\oplus(b_2\cdot p_2)\oplus(b_3\cdot p_3)\oplus(b_4\cdot p_4)\oplus(b_5\cdot p_5)\oplus(b_6\cdot p_6)\oplus(b_7\cdot p_7)]\oplus v_0\\
b'_1&=[(b_0\cdot p_7)\oplus(b_1\cdot p_0)\oplus(b_2\cdot p_1)\oplus(b_3\cdot p_2)\oplus(b_4\cdot p_3)\oplus(b_5\cdot p_4)\oplus(b_6\cdot p_5)\oplus(b_7\cdot p_6)]\oplus v_1\\
b'_2&=[(b_0\cdot p_6)\oplus(b_1\cdot p_7)\oplus(b_2\cdot p_0)\oplus(b_3\cdot p_1)\oplus(b_4\cdot p_2)\oplus(b_5\cdot p_3)\oplus(b_6\cdot p_4)\oplus(b_7\cdot p_5)]\oplus v_2\\
b'_3&=[(b_0\cdot p_5)\oplus(b_1\cdot p_6)\oplus(b_2\cdot p_7)\oplus(b_3\cdot p_0)\oplus(b_4\cdot p_1)\oplus(b_5\cdot p_2)\oplus(b_6\cdot p_3)\oplus(b_7\cdot p_4)]\oplus v_3\\
b'_4&=[(b_0\cdot p_4)\oplus(b_1\cdot p_5)\oplus(b_2\cdot p_6)\oplus(b_3\cdot p_7)\oplus(b_4\cdot p_0)\oplus(b_5\cdot p_1)\oplus(b_6\cdot p_2)\oplus(b_7\cdot p_3)]\oplus v_4\\
b'_5&=[(b_0\cdot p_3)\oplus(b_1\cdot p_4)\oplus(b_2\cdot p_5)\oplus(b_3\cdot p_6)\oplus(b_4\cdot p_7)\oplus(b_5\cdot p_0)\oplus(b_6\cdot p_1)\oplus(b_7\cdot p_2)]\oplus v_5\\
b'_6&=[(b_0\cdot p_2)\oplus(b_1\cdot p_3)\oplus(b_2\cdot p_4)\oplus(b_3\cdot p_5)\oplus(b_4\cdot p_6)\oplus(b_5\cdot p_7)\oplus(b_6\cdot p_0)\oplus(b_7\cdot p_1)]\oplus v_6\\
b'_7&=[(b_0\cdot p_1)\oplus(b_1\cdot p_2)\oplus(b_2\cdot p_3)\oplus(b_3\cdot p_4)\oplus(b_4\cdot p_5)\oplus(b_5\cdot p_6)\oplus(b_6\cdot p_7)\oplus(b_7\cdot p_0)]\oplus v_7
\end{aligned}
$$

having $p = p_0p_1p_2p_3p_4p_5p_6p_7$ as a load pattern consisting of {10001111} for the affine transformation and {00100101} for the inverse affine transformation and having v as a load

vector $= v_0v_1v_2v_3v_4v_5v_6v_7$ consisting of {11000110} for the affine transformation and {10100000} for the inverse affine transformation.

Satoh et al. teaches the affine transformation equations in matrix form in the top left corner of Fig. 1, but fails to explicitly teach the inverse affine transformation equations.

However, AAPA teaches the use of ROM for a look-up table (see page 4 lines 2-3) and teaches the equations (in matrix form) (see page 4 numerals 1.5 and 1.6).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to store the lookup table of Satoh et al. in ROM and for the circuit to implement the equations.

Motivation, as recognized by one of ordinary skill in the art, to do so would have been to allow the values of the table to be read but not changed and for the system to implement both AES/Rijndael encryption and decryption (see AAPA page 4).

14. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Satoh et al. as applied to claim 4 above, in view of Jarvinen et al. (A fully Pipelined Memoryless 17.8 Gbps AES-128 Encryptor".

As per claim 8, Satoh et al. fails to explicitly disclose the apparatus comprises a plurality of instances of a data processing module arranged in a data processing pipeline.

However, Jarvinen et al. teaches the use of pipelining in an AES system (see page 207 right column).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to pipeline the processes of the Satoh et al. system.

Motivation to do so would have been to increase the throughput of the system (see page 207 right column).

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Roselse and Van Buer teach methods of AES encryption with affine transformations and Rodrigues-Henriquez teaches a method of combining the affine and inverse affine transformations to increase the speed of the system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Pyzocha/
Examiner, Art Unit 2137